CNSS Instruction 4013
March 2004

NATIONAL INFORMATION

ASSURANCE TRAINING STANDARD

FOR

SYSTEM ADMINISTRATORS (SA)

Awareness, Training and Education (AT&E) are cost-effective methods of improving organizational Information Assurance (IA). In times of ever-contracting budgets, it is difficult to persuade management to spend money on security and training activities that have no direct impact on the organizational bottom line. This paper describes the process used to aid in the systematic development of training to serve as the first line of defense in Information Assurance (IA). In addition, it describes how these materials are applicable to your organizational long-range plans.

This document provides minimum standards for administrators of national security systems. It also may offer guidelines for administrators of unclassified systems. Your department or agency may require a more stringent implementation.

Committee on National Security Systems

NATIONAL MANAGER

FOREWORD

Since the September 11th terrorist attacks against the sovereignty of the United States and its people, both the President and the Congress have redoubled their efforts to underpin the nation's security. The following guidance, reflecting their support, is intended to assist all federal agencies and private sector entities in protecting their information systems. Only through diligence and a well-trained workforce will we be able to adequately defend the nation's vital information resources.

CNSSI No. 4013 is effective upon receipt. It replaces the National Training Standard for System Administrators in Information Systems Security (INFOSEC), dated August 1997, which should be destroyed.

This instruction establishes the minimum course content or standard for the development and implementation of Information Assurance (IA) training for system administrators (SAs). Please check with your agency for applicable implementing documents.

Additional copies of this instruction can be obtained on the CNSS Website www.nstissc.gov or by contacting the office at the address below.

NATIONAL SECURITY AGENCY
CNSS SECRETARIAT
ATTN: I01C STE 6716
FORT GEORGE G. MEADE, MD 20755-6716

/s/

MICHAEL V. HAYDEN
Lieutenant General, USAF

SYSTEM ADMINISTRATOR

NATIONAL INFORMATION ASSURANCE (IA)

TRAINING STANDARD FOR SYSTEM ADMINISTRATORS

SECTION I – PURPOSE

1. This instruction establishes the minimum training standard for the development and implementation of Information Assurance (IA) training for System Administrators (SAs).

SECTION II – APPLICABILITY

2. The President's National Strategy to Secure Cyberspace, Feb 03; National Security Telecommunications and Information Systems Security Directive (NSTISSD) No. 501, 16 Nov 92; Department of Defense Directive (DODD) 8000.1, 27 Feb 00; DoDD 8500.1, 24 Oct 02; Department of Defense Instruction (DODI) 8500.2, 6 Feb 03; and DODI 5200.40, 30 Dec 97 establish the requirements for DOD and other federal departments and agencies to implement training programs for IA professionals. As defined in NSTISSD 501, an IA professional is an individual responsible for the security oversight or management of national security systems during phases of the life cycle. Those directives and others are being implemented in a synergistic environment among departments and agencies, which are committed to vigorously satisfying these IA education and training requirements. The following document is a continuation in a series of minimum training and education standards being developed to assist departments and agencies in meeting their responsibilities in these areas (CNSSI [old NSTISSI] Nos. 4011, 4012, 4014, 4015, and 4016). Implementing the training outlined in this document concomitantly with the above NSTISSIs/CNSSIs will fulfill IA training requirements articulated in NIST 800-16, as mandated by 5 C.F.R. Part 930. The definitions for words used in this instruction are derived from the National Information Assurance (IA) Glossary, NSTISSI No. 4009. Many references pertinent to this instruction may be found in ANNEX B.

3. The body of knowledge listed in this instruction was obtained from a variety of sources, *i.e.*, industry, government, and academia. ANNEX A lists the minimal IA

performance standard for a SA. The APPENDIX provides a series of ancillary, platform specific security features and procedures.

4. This instruction is applicable to all departments and agencies of the U.S. Government and their contractors responsible for the development and implementation of IA training for SAs.

SECTION III - RESPONSIBILITIES

5. Heads of U.S. Government departments and agencies shall ensure that SAs (or their equivalents) are trained to the level of proficiency outlined in this instruction, and that such training is provided to those requiring it at the earliest practicable date.

6. The National Manager shall:

- maintain and provide an IA training standard for SAs to U.S. Government departments and agencies
- ensure that appropriate IA training courses for SAs are developed
- assist other U.S. Government departments and agencies in developing and/or conducting IA training activities for SAs as requested
- maintain a national clearinghouse for training and education materials

Enclosures:
Annex A with Appendix
Annex B

ANNEX A

MINIMAL INFORMATION ASSURANCE (IA) PERFORMANCE STANDARD FOR SYSTEM ADMINISTRATORS (SA)

Job Functions

The IA functions of an SA are:

1) working closely with the Information Systems Security Officer (ISSO) to ensure the Information System (IS) or network is used securely
2) participating in the Information Systems Security incident reporting program
3) assisting the ISSO in maintaining configuration control of the systems and applications software
4) advising the ISSO of security anomalies or integrity loopholes
5) administering, when applicable, user identification or authentication mechanism of the IS or network.

Terminal Objective:

ENTRY LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to describe and apply the appropriate actions to manage and administer an IS in a secure manner. To be acceptable, the description and application must be in accordance with applicable IA regulations, policies, and guidelines.

INTERMEDIATE LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to explain and implement the appropriate actions to manage and administer an IS in a secure manner. To be acceptable, the explanation and implementation must be in accordance with applicable IA regulations, policies, and guidelines.

ADVANCED LEVEL: Given various scenarios and typical situations containing information systems security issues, the SA will be able to verify that the appropriate actions are implemented to manage and administer an IS in a secure manner. To be acceptable, verification must be in accordance with applicable IA regulations, policies, and guidelines.

List of performance items under competencies: *

E = entry level

I = intermediate level

A = advanced level

**Note: These levels are linearly hierarchical*

GENERAL BACKGROUND

The following items constitute a basic literacy necessary for a System Administrator to proceed through the course material.

Definitions for Entry Level SAs

Define access control	Define accountability policy
Define accreditation	Define application development control
Define alarms, signals and reports	Define attack actions
Define assurance	Define authentication
Define audit log	Define biometrics
Define automated security tools	Define certification
Define organizational/agency incident response team	Define change control
Define client-server	Define concepts of multilevel security
Define configuration control	Define configuration management
Define continuity planning	Define copyright protection and licensing
Define corrective actions	Define countermeasures
Define disaster recovery	Define documentation
Define EKMS (Electronic Key Management) systems	Define electronic records management
Define error log	Define EMSEC (Emanations Security)/TEMPEST (Short name referring to the investigation, study, and control of compromising emanations from IS equipment) security
Define incident response	Define firewalls
Define information operations	Define information availability
Define integrity	Define information ownership
Define Internet security	Define internal controls
Define KMI systems	Define intrusion

Definitions for Entry Level SAs

Define multilevel security	Define modes of operation
Define one-time passwords	Define object reuse
Define operational procedure review	Define operating system integrity
Define PKI (Public Key Infrastructure) systems	Define password management
Define privacy	Define policy
Define protected distribution systems	Define privileges
Define safeguard	Define privacy
Define security training requirements	Define risk management
Define separation of duties	Define security
Define software piracy	Define sensitive information marking
Define system software controls	Define single sign-on
Define system security architecture study	Define Trusted Network Interpretation
Define validation and testing policies	Define verification and validation process policies
Define zoning and zone of control ratings	

In addition, a Systems Administrator should be able to discuss the following terms before beginning the program of instruction.

Discussion for Intermediate Level SAs

Discuss access authorization	Discuss authentication mechanisms
Discuss client-server security	Discuss configuration management
Discuss continuity plan	Discuss countermeasures
Discuss criminal activity preparedness	Discuss data access
Discuss database integrity	Discuss database security features
Discuss disaster recovery	Discuss documentation
Discuss electronic records management	Discuss privileges
Discuss EMSEC/TEMPEST	Discuss housekeeping procedures
Discuss error log	Discuss security training requirements
Discuss formal approval	Discuss information management
Discuss incident response	Discuss intrusion detection
Discuss information operations	Discuss major operating system security features
Discuss intrusion deterrents	Discuss network security software
Discuss levels of safeguards assurance	Discuss principle elements of security training
Discuss modes of operation	Discuss operating system security features
Discuss object reuse	Discuss privacy

Discussion for Intermediate Level SAs

Discuss objectives of security reviews	Discuss safeguard corrective actions
Discuss policy enforcement	Discuss different levels of countermeasures
Discuss risk management	Discuss objectives of security inspections
Discuss security inspections	

In each of the competency areas listed below, the SA shall perform the following functions at the levels indicated:

FUNCTION ONE – SECURE USE

Working closely with the Information Systems Security Officer (ISSO) to ensure the information systems or network is used securely.

A. General Security Policy

1. Accountability

E – Define organizational accountability policies
E – Outline accountability process/program
I – Discuss organizational accountability policies
I – Explain organizational accountability policies
I – Implement organizational accountability policies
A – Verify implementation of organizational accountability policies

2. Accreditation

E – Define accreditation
I – Discuss accreditation
I – Explain accreditation
I – Implement accreditation plan/process

3. Architecture

E – Define system security architecture
E – Identify appropriate security architecture for use in assigned IS
E – Address system security architecture study
I – Discuss system security architecture
I – Explain system security architecture

4. Assessment

E – Define assessments for use during certification of information systems
I – Discuss assessments for use during certification of information systems
I – Explain assessments for use during certification of information systems
A – Prepare assessments for use during certification of information systems

5. Assurance

E – Define assurance
I – Explain assurance
I – Discuss assurance

6. Availability/Integrity/Confidentiality/Authentication/Non-repudiation

E – Define concepts of availability, integrity, confidentiality, authentication, and non-repudiation
I – Discuss concepts of availability, integrity, confidentiality, authentication, and non-repudiation
I – Explain concepts of availability, integrity, confidentiality, authentication, and non-repudiation

7. Certification

E – Define certification policies as related to organizational requirements
I – Discuss certification policies as related to organizational requirements
I – Explain certification policies as related to organizational requirements

8. NSTISSP 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products

E – Identify NSTISSP 11 (Common Criteria) policies
I – Discuss NSTISSP 11 (Common Criteria) policies
I – Explain NSTISSP 11 (Common Criteria) policies

9. Configuration Control

E – Define configuration control (management)
I – Discuss configuration control (management)
I – Explain configuration control (management)
I – Comply with configuration management
I – Implement configuration control
I – Maintain configuration control
A – Verify implementation of configuration control

10. Custodian

E – Define resource custodian
E – Identify information resource custodian
I – Discuss resource custodian

11. Defense in Depth

E – Define defense in depth
E – Give examples of defense in depth methods
E – Give examples of defense in depth policy
I – Discuss defense in depth
I – Explain defense in depth

12. Document

E – Identify DoDD 8500.1 policies (or appropriate civil agency guidance)
I – Locate DoDD 8500.1 policies (or appropriate civil agency guidance)
I – Discuss DoDD 8500.1 policies (or appropriate civil agency guidance)
I – Explain DoDD 8500.1 policies (or appropriate civil agency guidance)

13. Domains

E – Define security domains as applicable to organizational policies
E – Describe security domains as applicable to organizational policies
I – Explain security domains as applicable to organizational policies

14. E-Mail

E – Define organizational e-mail privacy policies
I – Discuss organizational e-mail privacy policies
I – Explain organizational e-mail privacy policies
I – Implement organizational e-mail privacy policies
A – Verify implementation of organizational e-mail privacy policies

15. Wireless Security

E – Identify organizational wireless security policy
I – Discuss organizational wireless security policy

16. EMSEC/TEMPEST (Emanations Security/Short name referring to the investigation, study, and control of compromising emanations from IS equipment)

E – Define EMSEC/TEMPEST security policies
E – Describe EMSEC/TEMPEST control policies
E – Identify EMSEC/TEMPEST control policies
E – Identify EMSEC/TEMPEST security policies
I – Discuss EMSEC/TEMPEST control policies
I – Discuss EMSEC/TEMPEST security policies
I – Explain EMSEC/TEMPEST control policies
I – Explain EMSEC/TEMPEST security policies
I – Implement EMSEC/TEMPEST control policies
I – Implement EMSEC/TEMPEST security policies
A – Verify implementation of EMSEC/TEMPEST control policies
A – Verify implementation of EMSEC/TEMPEST security policies

17. Ethics

I – Discuss security policies relating to ethics
I – Explain security policies relating to ethics

18. FAX

E – Describe relevant FAX security policies

19. Generally Accepted Security Principles

E – Define generally accepted systems security principles

I – Discuss generally accepted systems security principles
I – Explain generally accepted systems security principles
A – Comply with generally accepted systems security principles

20. Goals/Mission/Objectives

E – Define goals, mission, and objectives of the organization
I – Discuss goals, mission, and objectives of the organization
I – Explain goals, mission, and objectives of the organization

21. Incident Response

E – Describe incident response policies
I – Discuss incident response procedure
I – Explain incident response policies
I – Implement incident response policies and procedures

22. Information Assurance

E – Define organizational Information Assurance (IA) policies
I – Discuss organizational policies
I – Explain organizational IA policies
I – Implement organizational IA policies
A – Verify implementation of organizational IA policies

23. Information Operations [DOD Organizations Only]

E – Define information operations
E – Describe information operations
E – Support information operations
I – Explain information operations

24. Internet Security

E – Describe organizational policies relevant to Internet security

25. Law Enforcement

E – Identify law enforcement interfaces
E – Describe law enforcement interfaces
I – Discuss law enforcement interfaces
I – Explain law enforcement interfaces

26. Marking

E – Define policies relating to marking of classified, unclassified and sensitive information
I – Discuss policies relating to marking of classified, unclassified, and sensitive information
I – Explain policies relating to marking of classified, unclassified, and sensitive information
I – Implement policies relating to marking of classified, unclassified, and sensitive information

A – Verify implementation of policies relating to marking of classified, unclassified, and sensitive information

27. Monitoring

E – Comply with legal aspects of monitoring
E – Ensure legal aspects of monitoring are enforced

28. Multi-Level Security

E – Describe multiple secure levels
E – Identify fundamental concepts of multilevel security
E – Define fundamental concepts of multilevel security
E – Describe fundamental concepts of multilevel security
I – Discuss multiple secure level
I – Discuss fundamental concepts of multilevel security
I – Explain fundamental concepts of multilevel security
I – Explain multiple secure levels
I – Implement fundamental concepts of multilevel security

29. Network

E – Describe computer network defense
E – Describe policies relevant to network security
E – Describe wide area network (WAN) security policies
I – Discuss computer network defense
I – Discuss organizational area network (LAN) security as related to organizational policies
I – Discuss WAN security policies
I – Explain computer network defense
I – Explain organizational area network (LAN) security as related to organizational policies
I – Explain WAN security policies
I – Implement WAN security policies
A – Verify implementation of WAN security policies

30. Operating System

E – Define functional requirements for operating system integrity
I – Discuss functional requirements for operating system integrity
I – Explain functional requirements for operating system integrity
I – Implement functional requirements for operating system integrity
A – Verify implementation of functional requirements for operating system integrity

31. Operations Security (OPSEC)

I – Discuss operations security (OPSEC) in conformance with organizational policies
I – Explain OPSEC in conformance with organizational policies
I – Implement OPSEC in conformance with organizational policies
A – Verify implementation of OPSEC in conformance with organizational policies

32. Ownership

E – Define information ownership of data held under his/her cognizance
E – Identify information ownership of data held under his/her cognizance
E – Identify information resource owner
I – Discuss information ownership of data held under his/her cognizance
I – Explain information ownership of data held under his/her cognizance

33. Physical Security

E – Define physical security
I – Discuss physical security policies
I – Explain physical security policies

34. Records Management

E – Define records management
E – Describe organizational security policies relative to electronic records management
I – Discuss records management
I – Explain records management

35. Secure Systems Operations

I – Discuss organizational policies relating to secure systems operations

36. Security Policy

I – Discuss significant agency specific security policies

37. Security Tools

E – Define automated security tools
I – Describe automated security tools
I – Explain automated security tools

38. Sensitivity

E – Define information sensitivity
E – Describe information sensitivity in relation to organizational policies
E – Explain information sensitivity
I – Discuss information sensitivity

39. Separation of Duties

E – Define separation of duties
E – Explain separation of duties
E – Define organizational policies relating to separation of duties
I – Discuss organizational policies relating to separation of duties
I – Explain organizational policies relating to separation of duties
I – Implement organizational policies relating to separation of duties
A – Verify implementation of organizational policies relating to separation of duties

40. System Security

E – Identify systems security standards policies

41. Information Technology Security Evaluation Criteria (ITSEC)

E- Identify Information Security Technology Security Evaluation Criteria (ITSEC) policies

42. Testing

E – Define testing policies
I – Discuss testing policies
I – Explain testing policies
I – Implement testing policies
A – Verify implementation of validation and testing policies

43. Validation/Verification

E – Define validation policies
E – Identify verification and validation process policies
I – Discuss validation policies
I – Discuss verification and validation process policies
I – Explain validation policies
I – Explain verification and validation process policies
I – Implement validation policies
I – Implement verification and validation process policies
A – Verify implementation of validation policies
A – Verify implementation of verification and validation process policies

44. Workstation

E – Describe workstation security policies
I – Discuss workstation security policies
I – Explain workstation security policies
I – Implement workstation security policies
A – Verify implementation of workstation security policies

45. Zone

E – Define zone of control
E – Define zoning
E – Describe zoning and zone of control policies
I – Discuss zoning and zone of control policies
I – Explain zoning and zone of control policies
I – Implement zoning and zone of control policies
A – Verify zoning and zone of control policies

B. General Procedures

1. Network Software

E – Define transport control protocol/internet protocol (TCP/IP)
E – Define transport layer security (*i.e.,* secure socket layer [SSL])
E – Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
E – Define virtual private network (VPN) (*i.e.*, SSH2, SOCKS)

E – Describe secure e-mail (*i.e.*, PGP, S/MIME)
E – Describe secure systems operations procedures
E – Describe transport control protocol/internet protocol (TCP/IP)
E – Describe transport layer security (*i.e.,* secure socket layer [SSL]
E – Describe tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
E – Describe virtual private network (VPN) (*i.e.*, SSH2, SOCKS)
I – Explain network components (hardware, firmware, software, and media)
I – Explain secure e-mail (*i.e.*, PGP, S/MIME)
I – Explain the principles of network security procedures
I – Explain transport layer security (*i.e.,* secure socket layer [SSL])
I – Explain tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
I – Explain virtual private network (VPN) (*i.e.*, SSH2, SOCKS)
I – Implement transport layer security (*i.e.,* secure socket layer [SSL])
A – Verify implementation of transport layer security (*i.e.,* secure socket layer [SSL])

2. Aggregation

E – Define aggregation
E – Describe aggregation
I – Discuss aggregation
I – Explain aggregation

3. Application Vulnerabilities

E – Describe application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
E – Describe application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
E – Describe application and system vulnerabilities and threats -- server-based
E – Describe application and system vulnerabilities and threats -- mainframe
E – Describe application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan horses, trap doors, viruses, worms)
I – Explain application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
I – Explain application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
I – Explain application and system vulnerabilities and threats -- server-based
I – Explain application and system vulnerabilities and threats -- mainframe
I – Explain application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan horses, trap doors, viruses, worms)

4. Architecture

E – Address system security architecture study
I– Explain system security architecture study

5. Assessment

E – Prepare assessments for use during certification of information systems
I – Explain assessments used during system certification process

6. Automated Tools

I – Explain expert system tools (*i.e.*, audit reduction and intrusion detection) available
I – Identify expert system tools (*i.e.*, audit reduction and intrusion detection) available
I – Use expert system tools (*i.e.*, audit reduction and intrusion detection) available

7. Organizational/Agency Systems Emergency Response Team

E – Identify organizational/agency systems emergency response team
E – Report security issues to organizational/agency systems emergency response team
I – Implement and distribute organizational/agency systems emergency response team reports and advisories
I – Explain organizational/agency systems emergency response team role

8. Database

E – Define data mining
E – Define databases and data warehousing vulnerabilities, threats and protections
E – Describe data mining
E – Describe databases and data warehousing vulnerabilities, threats and protections
I – Explain data mining
I – Explain databases and data warehousing vulnerabilities, threats and protections

9. EMSEC/TEMPEST

E – Define EMSEC/TEMPEST security procedures
E – Identify certified EMSEC/TEMPEST technical authority (CTTA)
E – Identify EMSEC/TEMPEST security procedures
I – Discuss EMSEC/TEMPEST security procedures
I – Explain EMSEC/TEMPEST security procedures

10. End Systems

E – Define end systems (*i.e.*, workstations, notebooks, PDA [personal digital assistant], smartphones, etc.)
E – Describe end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
I – Explain end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
I – Explain threats/vulnerabilities of end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)
I – Identify threats/vulnerabilities of end systems (*i.e.*, workstations, notebooks, PDA, smartphones, etc.)

11. Facility Management

E – Practice facility management procedures
I – Explain importance of sound facility management procedures
I – Implement facility management procedures
A – Verify implementation of facility management procedures

12. FAX

E – Describe FAX security policies/procedures
E – Practice FAX security policies/procedures

I – Implement FAX security policies/procedures
A – Verify implementation of FAX security policies/procedures

13. Housekeeping

E – Define housekeeping procedures
E – Describe housekeeping procedures
E – Perform housekeeping procedures
I – Explain housekeeping procedures

14. Inference

E – Define Inference
E – Describe Inference
I – Explain Inference

15. Information States

E – Define information states procedures
E – Describe information states procedures
A – Distinguish among information states procedures

16. Internet

E – Define Internet security procedures
I – Discuss Internet security procedures
I – Explain Internet security procedures
I – Implement Internet security procedures
A – Verify implementation of Internet security procedures

17. Investigations

E – Assist in investigations as requested

18. IPSEC

E – Define IPSEC authentication and confidentiality
E – Describe IPSEC authentication and confidentiality
I – Explain IPSEC authentication and confidentiality

19. Marking

E – Perform marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
I – Discuss marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
I – Explain marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
I – Implement marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information - Standard Forms) as an example
A –Verify implementation of marking of sensitive information procedures (defined in C.F.R. 32 Section 2003, National Security Information – Standard Forms) as an example

20. Multi-Level Security

E – Define multilevel security
I – Discuss multilevel security
I – Explain multilevel security
I – Apply multilevel security

21. Network, General

E – Define network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
E – Define network components (hardware, firmware, software, and media)
E – Define network layer security
E – Define network protocols
E – Define network types
E – Define wireless security
E – Describe network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
E – Describe network components (hardware, firmware, software, and media)
E – Describe network layer security
E – Describe network protocols
E – Describe network types
E – Describe WAN security procedures
E – Describe wireless security
E – Discuss network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
E – Practice WAN security procedures
I – Explain network architecture/topologies (*i.e.*, ETHERNET, FDDI, bus, star, mesh, etc.)
I – Explain network layer security
I – Explain network types
I – Explain wireless security
I – Implement network security procedures
I – Implement secure data communications
I – Implement secure voice and facsimile communications
I – Implement WAN security procedures
A – Verify implementation of network security procedures
A – Verify implementation of WAN security procedures

22. Network Hardware

E – Define cable characteristics (*i.e.*, twisted pair, fiber)
E – Define concentrators
E – Define front-end processors, hubs, modems, multiplexers
E – Define gateways and routers
E – Define patch panels
E – Define routers
E – Define switches

E – Describe cable characteristics (*i.e.*, twisted pair, fiber)
E – Describe concentrators
E – Describe front-end processors, hubs, modems, multiplexers
E – Describe gateways and routers
E – Describe patch panels
E – Describe routers
E – Describe switches
E – Identify gateways and routers
I – Explain cable characteristics (*i.e.*, twisted pair, fiber)
I – Explain concentrators
I – Explain front-end processors, hubs, modems, multiplexers
I – Explain gateways and routers
I – Explain patch panels
I – Explain routers
I – Explain switches
I – Implement gateways and routers

23. Network Software

E – Define firewall architecture (*i.e.*, bastion host, DMZ)
E – Define firewall technology (*i.e.*, packet filtering, data inspection)
E – Define secure e-mail (*i.e.*, PGP, S/MIME)
E – Describe firewall architecture (*i.e.*, bastion host, DMZ)
E – Describe firewall technology (*i.e.*, packet filtering, data inspection)
E – Describe secure e-mail (*i.e.*, PGP, S/MIME)
E – Identify firewall architecture (*i.e.*, bastion host, DMZ)
E – Identify firewall technology (*i.e.*, packet filtering, data inspection)
E – Identify secure e-mail (*i.e.*, PGP, S/MIME)
I – Explain firewall architecture (*i.e.*, bastion host, DMZ)
I – Explain firewall technology (*i.e.*, packet filtering, data inspection)
I – Explain secure e-mail (*i.e.*, PGP, S/MIME)
I – Implement firewall architecture (*i.e.*, bastion host, DMZ)
I – Implement firewall technology (*i.e.*, packet filtering, data inspection)
I – Implement secure e-mail (*i.e.*, PGP, S/MIME)

24. Objects

E – Define object reuse
E – Define polyinstantiation
E – Describe object reuse
E – Describe polyinstantiation
I – Explain object reuse
I – Explain polyinstantiation

25. Operating System

E – Define operating systems security procedures
E – Describe operating system integrity procedures
E – Perform operating systems security procedures

I – Explain operating systems security procedures
I – Implement operating systems security procedures
A – Verify implementation of operating systems security procedures

26. OSI (Open Systems Interconnect)

E – Define application layer security protocols (*i.e.,* secure electronic transactions, secure hypertext, secure remote procedure call)
E – Define data link layer security
E – Define network layer security
E – Define OSI model
E – Define transport control protocol/ internet protocol (TCP/IP)
E – Define transport layer security (*i.e.,* secure socket layer [SSL])
E – Define tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
E – Describe application layer security protocols (*i.e.,* secure electronic transactions, secure hypertext, secure remote procedure call)
E – Describe data link layer security
E – Describe network layer security
E – Describe OSI model
E – Describe presentation layer
E – Describe session layer
E – Describe physical layer
E – Describe transport control protocol/ internet protocol (TCP/IP)
E – Describe transport layer security (*i.e.,* secure socket layer [SSL])
I – Explain application layer security protocols (*i.e.,* secure electronic transactions, secure hypertext, secure remote procedure call)
I – Explain data link layer security
I – Explain network layer security
I – Explain network protocols
I – Explain OSI model
I – Explain transport control protocol/ internet protocol (TCP/IP)
I – Explain tunneling protocol (PPTP), layer 2 tunneling protocol (l2tp)
I – Implement application layer security protocols (*i.e.,* secure electronic transactions, secure hypertext, secure remote procedure call)
I – Implement data link layer security
I – Implement network layer security
I – Implement transport layer security (*i.e.,* secure socket layer [SSL])

27. Rainbow Series*

E – Describe purpose and contents of National Computer Security Center TG-005, Trusted Network Interpretation (TNI) or Red Book as examples
*N.B. Given that many have been trained using the Rainbow Series and given the historical context of Rainbow Series data, this body of information remains invaluable in lieu of a more current, national-level body of guidance. See below.

28. NSTISSAM COMPUSEC/1-99

E – Describe purpose and contents of NSTISSAM COMPUSEC/1-99, Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation

29. Security Procedures

E – Define organizational security procedures
E – Assist in organizational security procedures

30. Security tools

E – Define automated security tools
E – Describe automated security tools
I – Explain automated security tools

31. Vulnerability and Threat

E – Address application and system vulnerabilities and threats – mainframe
E – Address application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
E – Address application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
E – Address application and system vulnerabilities and threats -- server-based
E – Address application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)
E – Define application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
E – Define application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
E – Define application and system vulnerabilities and threats -- server-based
E – Define application and system vulnerabilities and threats -- mainframe
E – Define application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)
E – Describe application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
E – Describe application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
E – Describe application and system vulnerabilities and threats -- server-based
E – Describe application and system vulnerabilities and threats -- mainframe
E – Describe application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)
I – Explain application and system vulnerabilities and threats -- web-based (*i.e.*, XML, SAML)
I – Explain application and system vulnerabilities and threats -- client-based (*i.e.*, applets, active-X)
I – Explain application and system vulnerabilities and threats -- server-based

I – Explain application and system vulnerabilities and threats -- mainframe
I – Explain application and system vulnerabilities and threats -- malicious code (*i.e.*, Trojan Horses, trap doors, viruses, worms)

32. Zone

I – Explain zoning and zone of control procedures

C. General Awareness, Training and Education (AT&E)

Awareness, Training and Education (AT&E)

E – Describe attack actions as training issues
E – Identify sources of AT&E materials
I – Discuss the objectives of security inspections as a training issue
I – Discuss the objectives of security reviews as a training issue
I – Discuss the principle elements of security training
I – Distinguish among education, training, literacy and awareness
I – Explain attack actions addressed in training
I – Explain threat in its application to education, training, and awareness
I – Give examples of security awareness
I – Give examples of security training
I – Implement awareness materials as part of job
A – Verify implementation of awareness materials as part of job

D. General Countermeasures and Safeguards

1. Assessment

I – Prepare assessments for use during certification of information systems
I – Evaluate assessments used during certification of information systems

2. AT&E

E – Recognize awareness, training, and education (AT&E) as a countermeasure
I – Implement AT&E as a countermeasure

3. Backup

E – Define backup critical information
I – Identify critical information
I – Discuss backup critical information
I – Explain backup critical information

4. COMSEC

E – Identify national COMSEC manager (Custodian)
E – Identify organizational COMSEC manager (Custodian)
E – List national COMSEC policies
E – List national COMSEC procedures
I – Explain SA COMSEC procedures

5. Countermeasures

E – Describe what is meant by countermeasures
I – Discuss different levels of countermeasures assurance
I – Select countermeasures

6. Digest

E – Define message digests (*i.e.*, MD5, SHA, HMAC)
I – Discuss message digests (*i.e.*, MD5, SHA, HMAC)
I – Explain message digests (*i.e.*, MD5, SHA, HMAC)

7. Digital Signature

E – Define digital signatures
I – Discuss digital signatures
I – Explain digital signatures

8. Due Care

E – Define due care (due diligence)
I – Discuss due care (due diligence)
I – Explain due care (due diligence)

9. E-Mail

E – Describe e-mail privacy countermeasures
E – Describe e-mail privacy safeguards
I – Implement email security (*i.e.*, PGP, PEM)
I – Operate email security (*i.e.*, PGP, PEM)

10. EMSEC/TEMPEST

E – Define EMSEC/TEMPEST security countermeasures
E – Define EMSEC/TEMPEST security safeguards
I – Explain EMSEC/TEMPEST security countermeasures
I – Explain EMSEC/TEMPEST security safeguards
I – Implement EMSEC/TEMPEST security countermeasures
I – Implement EMSEC/TEMPEST security safeguards

11. Facilities

E – Define facility support systems (*i.e.*, fire protection and HVAC)
I – Discuss facility support systems (*i.e.*, fire protection and HVAC)
I – Explain Facility support systems (*i.e.*, fire protection and HVAC)
I – Implement Facility support systems (*i.e.*, fire protection and HVAC)
I – Operate facility support systems (*i.e.*, fire protection and HVAC)

12. Hardware

E – Define computing and telecommunications hardware/software
I – Discuss computing and telecommunications hardware/software
I – Explain computing and telecommunications hardware/software

13. Internet

E – Define internet security
I – Explain internet security
I – Implement internet security

14. Key

E – Define key creation/distribution
E – Define key recovery
E – Define key storage/destruction
E – Define PKI (Public Key Infrastructure) requirements
E – Submit requirements for key management within the system
I – Explain public key infrastructure (PKI) (*i.e.* certification authorities, etc)

15. Legal

E – Define legal requirements
I – Discuss legal requirements
I – Explain Legal requirements

16. Marking

E – Define marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
I – Discuss marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
I – Explain marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media
I – Implement marking, handling, storing, and destroying of classified, unclassified, and sensitive information & media

17. Media

E – Define magnetic media degaussing
E – Define marking, handling, storing, and destroying of sensitive information & media
E – Define media (*i.e.*, tape, paper or disks) management
E – Define secure data deletion for media reuse
I – Discuss magnetic media degaussing as an example of destruction
I – Discuss marking, handling, storing, and destroying of sensitive information & media
I – Discuss media (*i.e.*, tape, paper or disks) management
I – Discuss secure data deletion for media reuse
I – Explain magnetic media degaussing as an example of destruction
I – Explain marking, handling, storing, and destroying of sensitive information & media
I – Explain media (*i.e.*, tape, paper or disks) management
I – Explain secure data deletion for media reuse
I – Implement magnetic media degaussing as an example of destruction
I – Implement marking, handling, storing, and destroying of sensitive information & media
I – Implement secure data deletion for media reuse

18. Misuse

E – Define resource misuse prevention
I – Discuss resource misuse prevention
I – Explain resource misuse prevention
I – Implement resource misuse prevention

19. Non-Repudiation

E – Define digital non-repudiation
I – Discuss digital non-repudiation
I – Explain digital non-repudiation

20. Operations

E – Describe information operations
I – Discuss information operations

21. Privacy

E – Define privacy and protection
I – Discuss privacy and protection
I – Explain privacy and protection
I – Implement privacy and protection

22. Privilege

E – Define need-to-know/least privilege
E – Define operator/administrator privileges
I – Discuss need-to-know/least privilege
I – Discuss operator/administrator privileges
I – Explain need-to-know/least privilege
I – Explain operator/administrator privileges
I – Implement need-to-know/least privilege
I – Implement operator/administrator privileges

23. Record

E – Define record retention
I – Discuss record retention
I – Explain record retention
I – Implement record retention

24. Safeguards

E – Define safeguards used to prevent software piracy
E – Describe what is meant by safeguards
I – Discuss different levels of safeguards assurance

25. Separation of Duties

E – Describe separation of duties as a countermeasure
E – Explain separation of duties as a countermeasure
I – Discuss separation of duties as a countermeasure

26. Software Countermeasure

E – Define anti-virus systems
E – Define countermeasures used to prevent software piracy
I – Discuss anti-virus management
I – Discuss computing and telecommunications hardware/ software
I – Explain anti-virus management
I – Explain computing and telecommunications hardware/ software
I – Implement anti-virus management
I – Use anti-virus tools and procedures

27. Testing

E – Identify automated tools for security testing
I – Implement automated tools for security testing
A – Evaluate automated tools for security testing

28. Tools

E – Describe automated tools for security compliance
E – Describe automated tools for security test
I – Implement automated security tools
I – Implement automated tool for security test
I – Implement automated tools for security compliance
I – Operate automated security tools
I – Operate automated tool for security test
I – Operate automated tools for security compliance
A – Choose automated security tools

29. Zone

I – Explain what is meant by zoning and zone of control

E. Administrative Countermeasures/Safeguards

1. Alarm

E – Describe alarms, signals and reports
E – Identify alarms, signals and reports
E – Implement alarms, signals and reports

2. Assessment

E – Assist in preparing assessments
E – Prepare assessments for use during certification of information systems

3. System Test and Evaluation (ST&E)

E – Discuss System Test and Evaluation (ST&E) Plan and Procedures
E – Recommend revisions to System Test and Evaluation (ST&E) Plan and Procedures

4. Audit

E – Identify audit collection requirements
I – Enforce audit collection requirements
I – Implement audit trails and logging policies
A – Verify implementation of audit trails and logging policies

5. Certification

E – Discuss certification tools
E – Identify certification tools
E – Recommend use of specific certification tools

6. Control

E – Define application development control
E – Define system software controls
E – Differentiate security-related changes from non-security-related changes
E – Identify storage media protection and control
I – Implement change controls

7. Countermeasures

E – Identify countermeasures

8. Disposition

I – Discuss disposition of classified information
I – Implement disposition of media and data
I – Practice disposition of media and data
I – Use disposition of media and data
A – Verify implementation of disposition of media and data

9. Intrusion

I – Discuss intrusion detection resources and policies
I – Implement intrusion detection policies
I – Use intrusion detection resources
A – Verify implementation of intrusion detection resources and policies

10. Key

I – Implement key management techniques
I – Use key management techniques

11. Labeling

I – Implement document labeling
I – Practice document labeling
I – Use document labeling
A – Verify implementation of document labeling

12. Password

E – Address password management with staff

E – Identify password management systems
E – Define password management

13. Privacy

I – Discuss privacy act provisions
I – Explain privacy act provisions
I – Implement privacy act provisions

14. Recovery

E – Address recovery procedures with staff
E – Describe disaster recovery procedures
I – Explain disaster recovery procedures
I – Implement disaster recovery procedures
A – Verify implementation of disaster recovery procedures

15. Safeguards

I – Discuss proper use of security safeguards

16. Separation of Duties

E – Define separation of duties
E – Evaluate separation of duties
E – Implement separation of duties

F. Operations Policies/Procedures

1. Assessment

E – Support assessments for use during certification of information systems

2. Countermeasures

E – Identify protective technologies
E – List protective technologies

3. Crime

E – Support anti-criminal activity preparedness planning (law enforcement)
I – Discuss anti-criminal activity preparedness planning (law enforcement)

4. Database

I – Explain database security features
I – Implement database security features
I – Maintain database security features
I – Use database security features
A – Verify implementation of database security features

5. Disposition

E – Identify disposition of media and data policies and procedures
I – Explain disposition of media and data policies and procedures
I – Implement disposition of media and data policies and procedures

I – Perform disposition of media and data policies and procedures
A – Verify implementation of disposition of media and data policies and procedures

6. Documentation

E – Describe documentation policy and procedures
I – Implement documentation policy and procedures
I – Use documentation policy and procedures
A – Verify implementation of documentation policy and procedures

7. Media

E – Identify storage media control policies and procedures
E – Identify storage media protection policies and procedures

8. Objects

I – Discuss object reuse policy and procedures
I – Implement object reuse policy and procedures

9. Privacy

E – Outline known means of keystroke monitoring

10. Recovery

E – Define disaster recovery policies and procedures
E – Describe disaster recovery policies and procedures
I – Implement disaster recovery policies and procedures
I – Use disaster recovery policies and procedures
A – Verify implementation of disaster recovery policies and procedures

11. Separation of Duties

E – Describe separation of duties policies and procedures
I – Implement separation of duties policies and procedures
I – Practice separation of duties policies and procedures
I – Use separation of duties policies and procedures
A – Verify implementation of separation of duties policies and procedures

12. Vendor

E – Facilitate vendor cooperation
E – Explain vendor cooperation

G. Contingency/Continuity of Operations

1. Backup

E – Outline security policy for backup procedures
I – Develop security policy for backup procedures

2. Certification

I – Prepare assessments for use during certification of information systems

3. Continuity/Contingency

E – Describe continuity/contingency planning
E – Prepare input to continuity/contingency plan
I – Discuss continuity/contingency plan
I – Exercise continuity/contingency plan
I – Implement continuity/contingency plan
A – Verify implementation of continuity/contingency plan
A – Write continuity/contingency plan
A – Test continuity/contingency plan
A – Evaluate continuity/contingency plan testing results

4. Recovery

E – Describe disaster recovery
E – Describe disaster recovery plan testing
E – Prepare input to recovery plan
I – Discuss disaster recovery planning
I – Exercise disaster recovery operations
I – Implement disaster recovery
I – Implement disaster recovery plan testing
I – Implement disaster recovery planning
I – Perform contingency operations
I – Perform disaster recovery
I – Perform disaster recovery planning
A – Verify implementation of disaster recovery plans, policies, and procedures
A – Verify implementation of disaster recovery plan testing
A – Verify implementation of disaster recovery planning
A – Evaluate disaster recovery plan exercise results
A – Write recovery plan
A – Include lessons-learned from disaster recovery test in new disaster recovery plan

FUNCTION 2 – INCIDENTS

Participating in the Information Systems Security incident reporting program

A. Policy and Procedures

1. Attack

I – Identify attack
I – Identify appropriate attack response
I – Implement attack response

2. Disposition

E – Address disposition procedures with staff

3. Due Care

E – Address questions from users about due care

4. Incident

E – Define incidents
E – Define breaches
E – Address unauthorized access incident reporting with staff
E – Define incident response
I – Discuss breaches
I – Discuss incident response
I – Discuss incidents
I – Enforce incident response policy/procedures
I – Explain incident response
I – Implement incident response
I – Implement incident response policy/procedures
A – Verify implementation of incident response policy/procedures are implemented
I – Discuss evidence preservation
I – Implement evidence preservation IAW legal guidance

5. Intrusion

E – Define intrusion detection
E – Address intrusion detection management with staff
I – Discuss intrusion detection
I – Implement intrusion detection
A – Verify implementation of intrusion detection is implemented

6. Legal

E – Assist appropriate authority in witness interviewing/interrogation
E – Assist in evidence identification/preservation

7. Reporting

E – Define reporting
I – Discuss reporting
I – Explain reporting

8. Response

I – Discuss attacks response

9. Violation

E – Define violations
I – Discuss violations
I – Explain violations

B. Operations Countermeasures/Safeguard

1. Alarm

I – Use alarms, signals, and reports

2. Attack

E – Identify an attack
A – Analyze an attack
A – Summarize an attack

3. Audit

I – Implement audit trails and logging policies
A – Verify implementation of audit trails and logging policies

4. Authentication

E – Address work force about authentication procedures
I – Implement authentication policies and procedures
A – Verify implementation of authentication policies and procedures

5. Organizational/Agency Systems Emergency Response Team

E – Describe the organizational/agency systems emergency/incident response team
I – Use the organizational/agency systems emergency/incident response team
I – Comply with procedures of the organizational/agency systems emergency/incident response team

6. Countermeasure

E – Assist in performing countermeasure/safeguard corrective actions
E – Describe countermeasures
I – Discuss countermeasure
I – Implement countermeasures
I – Use countermeasures
A – Perform countermeasures
A – Verify implementation of countermeasures

7. Incident

E – Address unauthorized access incident reporting with staff
E – Assist in incident response
I – Implement incident response
I – Report incident response
A – Perform incident response
A – Verify implementation of incident response

8. Intrusion

I – Implement intrusion detection
I – Monitor intrusion detection
I – Report intrusion
A – Perform intrusion detection
A – Verify implementation of intrusion detection
A – Verify implementation of intrusion detection posture

9. Legal

E – Assist appropriate authority in witness interviewing/interrogation

10. Safeguard

E – Describe safeguards
I – Discuss safeguard corrective actions
I – Implement safeguards
I – Use safeguards
A – Verify implementation of safeguards

C. Contingency Countermeasures/Safeguards

1. Alarms

I – Use alarms, signals, and reports

2. Availability

E – Define information availability

3. Correction

E – Identify examples of corrective actions

4. Countermeasures

I – Select countermeasures with ISSO

5. Incident

E – Address unauthorized access incident reporting with staff

6. Intrusion

E – Identify methods of intrusion detection

7. Safeguards

I – Select appropriate safeguards with ISSO

FUNCTION 3 -- CONFIGURATION

Assist the ISSO in maintaining configuration control of the systems and applications software.

Administrative Policies/Procedures

1. Access

I – Discuss access authorization
I – Implement access authorization
A – Verify implementation of access authorization

2. Approval To Operate (ATO)

I – Discuss formal approval to operate
I – Implement formal approval
A – Verify implementation of formal approval to operate

3. Authentication

E – Address authentication with staff
E – Address work force about authentication procedures

4. Biometrics

E – Address biometric access management with staff

5. Organizational/Agency Systems Emergency/Incident Response Team

E – Identify organizational/agency systems emergency/incident response team
I – Implement organizational/agency systems emergency/incident response team security reporting

6. Configure

E – Define change control policies
E – Define configuration control
E – Address configuration management with staff
E – Address staff about legal configuration restrictions
E – Adhere to configuration control
E – Monitor configuration control
I – Implement change control policies
I – Implement configuration control
I – Maintain configuration control
A – Verify implementation of change control policies

7. Copyright

E –Adhere to copyright protection and licensing
E – Define copyright protection and licensing
I – Implement copyright protection and licensing
A – Verify implementation of copyright protection and licensing

8. Documentation

I – Discuss documentation
I – Implement documentation
A – Verify implementation of documentation

9. Inspection

I – Discuss security inspections
I – Implement security inspections
A – Verify implementation of security inspection report recommendations

10. Install/Patch

E – Identify appropriate sources for updates and patches
I – Describe how to install multiple patches with a single batch file
I – Implement and manually install a patch from an appropriate source
I – Implement and verify a security patch or upgrade
I – Implement multiple patches with a single batch file
I – Implement operating system from appropriate source
A – Verify and manually install a patch from an appropriate source
A – Verify implementation of a security patch or upgrade
A – Verify implementation of multiple patches with a single batch file
A – Verify implementation of operating system from appropriate source

11. Logging

I – Describe the different categories of activities which may be logged

12. Management

E – Identify basic/generic management issues

13. Network

I – Explain network security software
I – Implement network security software
A – Verify implementation of network security software

14. Objects

I – Describe object reuse

15. Operation

E – Define operational procedure review
I – Implement operational procedure review
A – Verify implementation of operational procedure review

16. Password

E – Address password management with staff
I – Describe organizational password management policy

17. Policy

I – Discuss policy enforcement
I – Implement policy enforcement
A – Verify implementation of policy enforcement

18. Records

I – Explain electronic records management
I – Implement electronic records management
A – Verify implementation of electronic records management

19. Wireless

I – Describe organizational wireless use policy

FUNCTION 4 – ANOMALIES AND INTEGRITY

Advise the ISSO of security anomalies or integrity loopholes.

A. General Risk Management

1. Attack

E – Describe attack actions
E – Identify attack actions
I – Explain attack actions

2. Defense in Depth

I – Summarize defense in depth

3. EMSEC/TEMPEST

E – Define EMSEC/TEMPEST security as it relates to the risk management process
E – Describe EMSEC/TEMPEST security as it relates to the risk management process
I – Explain EMSEC/TEMPEST security as it relates to the risk management process

4. Internet

E – Describe ways to provide protection for Internet connections
I – Explain ways to provide protection for Internet connections

5. Legal

E –Assist in investigations as requested

6. Logging

E – Describe the different categories of activities which may be logged

7. Network

E – Describe wireless security
E – Describe LAN/WAN security
I – Explain wireless security
I – Explain LAN/WAN security

8. Operating System

E – Describe operating system integrity

9. Risk

I –Report risks to ISSO

10. Threat

E – Identify different types of threat
I – Report threats to ISSO

11. Zone

E – Describe on what zoning and zone of control ratings are based
I – Explain zoning and zone of control ratings

B. Access Control Safeguards

1. Access Control

E – Address access control software management with staff
E – Address work force about access control software management procedures
E – Define decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
E – Define discretionary access controls
E – Define mandatory access controls
E – Define security domain
E – Describe access control physical, logical, and administrative configurations
E – Describe access rights and permissions
E – Describe control techniques and policies (*i.e.*, discretionary, mandatory, and rule f least privilege
E – Identify access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
I – Explain access control attacks (brute force, dictionary, spoofing, denial of service, etc.)
I – Explain access control physical, logical, and administrative configurations
I – Explain access rights and permissions
I – Explain control techniques and policies (*i.e.*, discretionary, mandatory, and rule of least privilege decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
I – Explain identification and authentication techniques
I – Explain security domain
I – Explain single/multifactor authentication (knowledge based *i.e.*, password/pass phrase, one time, tokens/smart cards and characteristic based *i.e.*, biometrics)
I – Implement access control physical, logical, and administrative configurations

I – Implement access rights and permissions
I – Implement control techniques and policies (*i.e.*, discretionary, mandatory, and rule of least privilege
I – Implement decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
I – Implement security domain
A – Use security domain
A – Use decentralized/distributed -- single sign on (SSO) (*i.e.*, Kerberos)
A – Use remote access protocols (*i.e.*, PPP/CHAP/PAP/EAP)

2. Alarms

E – Demonstrate the ability to use alarms, signals, and reports
A – Use alarms, signals, and reports

3. Authentication

E – Describe centralized/remote authentication access controls
E – Describe identification and authentication techniques
E – Identify identification and authentication techniques
I – Explain centralized/remote authentication access controls
A – Use centralized/remote authentication access controls
A – Use single/multifactor authentication (knowledge based *i.e.*, password/pass phrase, one time, tokens/smart cards and characteristic based *i.e.*, biometrics)

4. Distribution System

E – Define protected distribution systems

5. Intrusion

I – Explain intrusion detection

6. Legal

E – Address staff about legal access restrictions
E – Assist in investigations as requested

7. Monitor

E – Define accountability and monitoring (*i.e.*, correction, alarms, audit trail)
E – Describe accountability and monitoring (*i.e.*, correction, alarms, audit trail)
I – Explain accountability and monitoring (*i.e.*, correction, alarms, audit trail)
I – Implement accountability and monitoring (*i.e.*, correction, alarms, audit trail)

8. Network

E – Identify network security software

9. Operating System

E – Describe operating system security features

10. Ownership

E – Describe data ownership and custodianship
I – Explain data ownership and custodianship

I – Implement data ownership and custodianship

11. Safeguards

E – Describe system security safeguards
I – Implement countermeasures to deter/mitigate attack threats (*i.e.,* malicious code, flooding, spamming)

C. Audit Policies and Procedures

1. Address

E – Address access management with staff

2. Alarms

I – Use alarms, signals, and reports in accordance with existing policies and procedures

3. Audit

I – Implement audit trails and logging policies
I – Summarize audit-related documentation
A – Verify implementation of audit trails and logging policies are implemented

4. Legal

E – Address staff about legal access restrictions
E – Assist in investigations as requested

5. Records

I – Discuss electronic records management relative to compliance with organizational policies and procedures

6. Separation of Duties

E – Describe situations in which separation of duties is appropriate or mandatory

D. Audit Countermeasures/Safeguards

1. Audit

I – Describe safeguards gained through use of audit trails
I – Identify countermeasures applicable to audit trail tampering

2. Legal

E – Assist in investigations as requested

E. Audit Tools

1. Audit

E – Define an error/audit log
E – Identify audit tools
E – Describe the major benefit gained through use of audit trails and logging policies
I – Explain capabilities offered by expert audit tools

I – Explain major benefits of auditing

2. Intrusion

E – Identify intrusion detection systems

3. Legal

E – Assist in investigations as requested

4. Operating Systems

E – Describe major operating system security features

5. Tools

I – Explain capabilities offered by expert security tools

F. Operations Management/Oversight

1. Audit

I – Explain error log
I – Use error log

2. Change Control

I – Implement management/oversight change controls
I – Use management/oversight change controls
A – Verify implementation of management/oversight change controls

3. Configuration Management

E – Describe configuration management

4. Integrity

I – Discuss database integrity
I – Discuss information management
I – Identify the key elements of information integrity

5. Legal

E – Assist in investigations as requested

6. Monitoring

E – Address monitoring management with staff

7. Records

I – Discuss electronic records management
I – Discuss electronic records oversight

8. Recovery

E – Describe disaster recovery management
E – Describe disaster recovery oversight
I – Implement disaster recovery management/oversight

I – Use disaster recovery management/oversight
A – Verify implementation of disaster recovery management/oversight

9. Risk

I – Explain risk management
I - Practice risk management

G. Configuration Management

1. Architecture

I – Explain how the security architecture is affected by assurance, trust, and confidence countermeasures; covert channels; EMSEC/TEMPEST; maintenance hooks and privileged programs; states attacks (*i.e.*, time of check / time of use); and timing attacks

2. Change Control

I – Implement change control policies
A – Interface with configuration control board

3. Disposition

I – Perform disposition of media and data
I – Practice disposition of classified info
I – Practice emergency destruction
I – Use disposition of classified info
I – Use emergency destruction

4. Integrity

I – Explain database integrity

5. Legal

E – Assist in investigations as requested

6. Media

E – Identify storage media protection and control procedures

7. Subjects and Objects

E – Define subjects and objects

8. Platforms

I – Explain the elements of technical platforms

9. Records

I – Explain electronic records management
I – Perform electronic records management

10. Trusted Computer Base (TCB)

E – Define trusted computer base (TCB) reference monitors and kernels

FUNCTION 5 -- ADMINISTRATION

Administering, when applicable, security mechanisms of an IS or network

A. Access Control Policies/Administration

1. Access Control

E – Address access control software management with staff
E – Address access management with staff
E – Address work force about access control software management procedures
E – Address work force about access management procedures
E – Address work force about account management procedures
E – Describe data access
I – Explain access control policies
I – Use network access controls as designed

2. Accounts

E – Address account management with staff
I – Perform account deletions

3. Authentication

E – Address authentication with staff
E – Address work force about authentication procedures

4. Awareness, Training and Education (AT&E)

I – Discuss requirements for security awareness, training, and education

5. Biometrics

E – Address biometric access management with staff

6. Compartments

I – Implement compartmented/partitioned mode
I – Explain compartmented/partitioned mode

7. Custodian

E – Identify information resource custodian

8. Disposition

E – Address disposition procedures with staff

9. Due Care

E – Address questions from users about due care

10. Legal

E – Address staff about legal access restrictions

E – Address staff about legal monitoring restrictions

11. Mode of Operation

E – Define modes of operation
E – Describe modes of operation
E – Identify the dedicated mode of operation
I – Use modes of operation

12. Monitoring

E – Outline known means of electronic monitoring

13. Owner

E – Identify information resource owner
E – Define information ownership

14. Password

E – Describe a method to force regular password changes and the limitations of the method

15. Separation of Duties

E – Describe separation of duties

16. Vendors

E – Facilitate vendor cooperation

17. Audit

E – Address work force about auditing and logging management procedures

B. Access Control Countermeasures

1. Awareness, Training and Education (AT&E)

I – Develop security training plan and materials for information system users
I – Discuss security education
I – Encourage employees to seek education in IA as a countermeasure
I – Monitor changing security education requirements for information system users

2. Authentication

E – Address work force about authentication procedures

3. Biometrics

E – Address biometric access management with staff

4. COMSEC Policy

E – List national COMSEC policies
E – List national COMSEC procedures
I – Discuss COMSEC procedures

5. Control

E – Define internal controls and security
I – Discuss internal controls and security

6. Countermeasures

E – Describe countermeasures
E – Define countermeasures
E – Give examples of countermeasures
I – Discuss countermeasures

7. Firewalls

I – Discuss network firewalls

8. Intrusion

E – Identify methods of intrusion detection
E – Address intrusion detection management with staff
E – Address staff about intrusion detection
E – Address staff about intrusion deterrents

9. Isolation and Mediation

E – Define isolation and mediation
I – Discuss isolation and mediation
I – Implement isolation and mediation
I – Monitor isolation and mediation

10. Key

E – Demonstrate knowledge of how to operate a KMI-enabled system
E – Submit requirements key management

11. Monitoring

E – Address monitoring management with staff
E – Address staff about monitoring and auditing intrusion detection policies
E – Address work force about monitoring management procedures

12. Network

E – Define network firewalls
E – Describe network security software

13. Password

E – Address password management with staff

14. Tools

I – Operate automated security tools
I – Operate automated tools for security compliance
A – Evaluate automated security tools
A – Evaluate automated tools for security compliance

C. Access Control Mechanisms

1. Access Control

E – Define discretionary access controls
E – Define mandatory access controls
E – Describe discretionary access controls
E – Describe mandatory access controls
I – Use access control software
I – Implement access control software

2. Audit

I – Use audit trails and logging policies
I – Implement audit trails and logging policies
I – Maintain audit trails and logging policies

3. Authentication

I – Implement authentication mechanisms
I – Discuss authentication mechanisms

4. Biometrics

E – Describe biometrics
I – Implement biometrics
I – Use biometrics

5. Database

I – Discuss database security features
I – Implement database security features

6. Isolation and Mediation

I – Implement isolation and mediation
I – Monitor isolation and mediation
I – Use isolation and mediation

7. Key

I – Use KMI applications
I – Use KMI products
I – Implement KMI applications
I – Implement KMI products

8. Operating System

I – Discuss operating system security features
I – Use operating system security features
I – Implement operating system security features
I – Maintain operating system security features

9. Password

E – Define one-time passwords
E – Define single sign-on
E – Describe one-time passwords
I – Use single sign-on
I – Implement single sign-on

10. Privilege

I – Discuss privileges

11. Security

I – Discuss client-server security
I – Use client-server security
I – Use database security features
I – Implement client-server security
I – Maintain client-server security

APPENDIX

PLATFORM SPECIFIC SECURITY FEATURES/PROCEDURES

Many platform or organization specific security features/procedures are ephemeral and should be defined by the agency, service, or organization employing the ISSO. The following list of knowledge items, contributed by a consortium of public/private sector interests, has been identified as high-frequency-of-change and is an example of constantly evolving best practices at the moment. Organizations should establish mechanisms to fold these types of items into their training implementations. They should be considered as ancillary to the primary training standard.

Windows Data		
W1		**Background Knowledge**
W1.01	K	Define "windows domain".
W1.02	K	Define "domain controller".
W1.03	K	Define "organizational user account".
W1.04	K	Define "domain user account".
W1.05	K	Define "computer account".
W1.06	K	Define "domain member" (or "member server").
W1.07	K	Define "NetBios name".
W1.08	K	Define "CIFS" (a.k.a."SMB")
W1.09	K	Define "shared folder".
W1.10	K	Define "NTFS" and "FAT".
W1.11	K	Define "registry".
W1.12	K	Describe some of the essential differences between the two main families of Microsoft operating systems: Windows 95/98/Me and Windows NT/2000/XP/.NET.
W1.13	K	Be familiar with the following Microsoft program: Active Directory Users and Computers MMC snap-in.
W1.14	K	Be familiar with the following Microsoft program: Certificates MMC snap-in.
W1.15	K	Be familiar with the following Microsoft program: Computer Management MMC snap-in.
W1.16	K	Be familiar with the following Microsoft program: DCPROMO.EXE
W1.17	K	Be familiar with the following Microsoft program: Event Viewer MMC snap-in.
W1.18	K	Be familiar with the following Microsoft program: IP Security Policies MMC snap-in.
W1.19	K	Be familiar with the following Microsoft program: IPCONFIG.EXE
W1.20	K	Be familiar with the following Microsoft program: IPSECCMD.EXE (on Windows XP/.NET)
W1.21	K	Be familiar with the following Microsoft program: IPSECPOL.EXE (on Windows 2000)

Windows Data		
W1.22	K	Be familiar with the following Microsoft program: Microsoft Management Console (MMC.EXE)
W1.23	K	Be familiar with the following Microsoft program: NBTSTAT.EXE
W1.24	K	Be familiar with the following Microsoft program: NET.EXE - for each relevant version of Windows
W1.25	K	Be familiar with the following Microsoft program: Network Monitor (NETMON.EXE)
W1.26	K	Be familiar with the following Microsoft program: REGEDIT.EXE
W1.27	K	Be familiar with the following Microsoft program: REGEDT32.EXE
W1.28	K	Be familiar with the following Microsoft program: SECEDIT.EXE
W1.29	K	Be familiar with the following Microsoft program: Security Configuration and Analysis MMC snap-in.
W1.30	K	Be familiar with the following Microsoft program: Security Templates MMC snap-in.
W1.31	K	Be familiar with the following Microsoft program: Task Manager (TASKMGR.EXE)
W1.32	K	Be familiar with the following Microsoft programs: TRACERT.EXE and compare it with ping -a IP.nu.mb.er
W1.33	K	Be familiar with the following Microsoft program: XCACLS.EXE
W1.34	K	Be familiar with the following non-Microsoft program: L0phtCrack
W1.35	K	Be familiar with the following non-Microsoft program: Legion
W1.36	K	Be familiar with the following non-Microsoft program: Nmap
W1.37	K	Be familiar with the following non-Microsoft program: DumpSec
W1.38	K	Be familiar with the following non-Microsoft program: WinDump
W1.39	K	Be familiar with WinPCap and how to install it
W1.40	K	Be familiar with the following non-Microsoft program: SuperCACLS
W1.41	K	Be familiar with the following Microsoft program: SRVINFO.EXE
W1.42	K	Be familiar with the following Microsoft program: HFNETCHK.EXE
W1.43	K	Be familiar with the following Microsoft program: IISLOCKD.EXE
W1.44	K	Define and contrast LM, NTLM and NTLMv2.
W1.45	S	Install Windows NT
W1.46	K	Describe the key security risks involved in the installation of Windows NT
W1.47	S	Install Windows 2000
W1.48	K	Describe the key security risks involved in the installation of Windows 2000
W1.49	S	Install Windows 98/95/ME
W1.50	K	Describe the key security risks involved in the installation of Windows 98/95/ME
W10		Delegation of Authority
W10.1	K	Describe Organizational Units in Active Directory.
W10.2	K	Define "Active Directory permission".
W10.3	K	Describe how Active Directory permissions on user accounts, computer accounts and Group Policy Objects can Be used to delegate authority over these objects.

Windows Data		
W10.4	S	Use the Delegation of Authority Wizard to give a group the ability to create, delete and modify the user accounts in an Organizational Unit, including the ability to reset passwords on user accounts in that Organizational Unit.
W10.5	S	Use Group Policy to add a global group to the organizational Administrators group on each computer in an Organizational Unit.
W10.6	S	Use Group Policy to give a global group additional user rights on all the computers in an Organizational Unit.
W11		**Automation and Scripting Support**
W11.1	K	Define "logon script".
W11.2	S	Deploy logon scripts for both current and legacy clients.
W11.3	K	Describe the variety of command-line tools and scripts that can be obtained from the Microsoft Resource Kit or managing security.
W11.4	S	Use Group Policy to automatically deploy startup, shutdown, logon and logoff scripts to computers throughout the organization.
W11.5	S	Use the Task Scheduler on organizational or remote systems for automating the execution of scripts or programs for security.
W2		**Domains and Trusts**
W2.1	K	Define "Active Directory forest".
W2.2	K	Describe trusts and the security consequences of (not) having trusts.
W2.3	K	Describe Active Directory database synchronization among domains in the forest, *i.e.*, describe domains and forests as "replication boundaries".
W2.4	K	Describe the security consequences of isolating users/computers in their own separate domain, whether that domain is in the forest or not.
W2.5	S	Install Active Directory on a server using DCPROMO.EXE.
W2.6	S	Configure explicit trust relationships.
W3		**Group Policy and Security Templates**
W3.01	K	Define "Group Policy".
W3.02	K	Describe the uses of Group Policy for security.
W3.03	S	Create and edit Group Policy Objects in Active Directory.
W3.04	K	Define "security template" as it pertains to Group Policy.
W3.05	S	Edit a security template using the Security Templates MMC snap-in.
W3.06	K	Describe the Security Configuration and Analysis (SCA) snap-in.
W3.07	K	Describe the SECEDIT.EXE tool.
W3.08	S	Audit the settings of a computer using the SCA snap-in.
W3.09	S	Audit the settings of a computer using SECEDIT.EXE.
W3.10	S	Configure a computer using the SCA snap-in.
W3.11	S	Configure a computer using SECEDIT.EXE.
W4		**User Accounts and Account Policies**
W4.01	K	Describe the role of user accounts and groups in the Windows security model, especially with respect to NTFS permissions, user rights, and auditing user behavior.

Windows Data		
W4.02	S	Create users and groups with the Active Directory Users and Computers snap-in.
W4.03	K	Define "strong password".
W4.04	K	Define "password hash".
W4.05	K	Define "CHAP" and "MSCHAP" password protocols
W4.06	K	Define "password policy".
W4.07	K	Describe the importance of enforcing a strong password policy.
W4.08	S	Configure password policy through Group Policy, including minimum password length, maximum password age, password history length, minimum password age, and password complexity requirements.
W4.09	S	Use a password-cracking tool, such as L0phtCrack, to audit the strength of users' passwords on a regular basis.
W4.10	K	Define "account lockout policy".
W4.11	K	Describe the issues surrounding an account lockout policy.
W4.12	S	Configure account lockout policy through Group Policy, including lockout threshold, lockout duration, and bad password count reset interval.
W5		**NTFS, Share and Registry Permissions**
W5.01	K	Define "NTFS file system".
W5.02	K	Describe NTFS permissions (DACLs) and audit settings (SACLs).
W5.03	S	Configure an NTFS permission on a folder or file with Windows Explorer.
W5.04	K	Describe how a user's final, cumulative permissions to a file are calculated, based on that user's various group memberships, when that file is accessed over the network through a shared folder on a volume formatted with NTFS.
W5.05	K	Describe how a user's being the "NTFS owner" of a file/folder affects what that user can do with that file/folder.
W5.06	S	Configure NTFS permissions through Group Policy.
W5.07	S	Convert a FAT file system to NTFS with CONVERT.EXE without destroying data.
W5.08	K	Define "shared folder".
W5.09	K	Describe the share permissions: Read, Change, Full Control, Deny.
W5.10	S	Edit a share permission on a folder with Windows Explorer.
W5.11	K	Define "registry".
W5.12	S	Edit registry keys and values with REGEDT32.EXE and REGEDIT.EXE.
W5.13	S	Edit the permissions on a registry key with REGEDT32.EXE
W5.14	S	Configure the permissions of registry keys through Group Policy.
W6		**Patches, Hotfixes and Service Packs**
W6.01	K	Define "service pack".
W6.02	K	Describe the effect and importance of applying the latest service pack for security and describe the risks of patching and the need for change control.
W6.03	S	Install a service pack using the graphical installation tool.
W6.04	S	Install a service pack hands-free with the necessary command-line switches.
W6.05	K	Define "slipstreaming a service pack during OS installation".

Windows Data		
W6.06	S	Extract and merge the files from a service pack into a folder where the operating system installation files have been copied ("-s" switch).
W6.07	K	Define "patch" (or "hotfix").
W6.08	S	Download and manually install a patch from Microsoft.
W6.09	K	Describe how to install multiple patches with a single batch file.
W6.10	K	Describe the capabilities of the Network Hotfix Checker (HFNETCHK.EXE) from Microsoft and the purpose of each of its command-line switches.
W6.11	S	Use HFNETCHK.EXE to determine which patches have not been applied to organizational or remote systems.
W7		**Auditing and Logging**
W7.01	K	Define "audit policy".
W7.02	K	Describe the different categories of activities which may be logged.
W7.03	S	Configure audit policy through Group Policy.
W7.04	K	Describe how to audit access to NTFS folders and files.
W7.05	S	Configure NTFS auditing on a folder or file with Windows Explorer.
W7.06	S	Configure NTFS auditing through Group Policy.
W7.07	S	Use Event Viewer to examine the audit logs on a organizational or remote system.
W7.08	S	Export an event log to a tab- or comma-delimited text file with Event Viewer.
W7.09	S	Import a textual log file into a database, spreadsheet or other tool which permits the consolidation and reconstruction of event log data.
W7.10	S	Filter and examine a consolidated event log to reconstruct the activities of a single user, computer or service.
W7.11	K	Describe the shortcomings of 1) using only Event Viewer for analyzing event logs, and 2) logging only to the organizational machine, *i.e.*, no syslog service.
W8		**Encryption Facilities: EFS and IPSec**
W8.01	K	Define "Encrypting File System (EFS)."
W8.02	S	Encrypt a folder using EFS with Windows Explorer or CIPHER.EXE.
W8.03	K	Define "EFS recovery agent."
W8.04	S	Export and delete the private key of the recovery agent from stand-alone computers.
W8.05	S	Change the recovery agent through Group Policy on computers which are domain members.
W8.06	K	Define "Internet Protocol Security (IPSec)."
W8.07	K	Describe the uses of IPSec for secure communications and Virtual Private Networking.
W8.08	S	Use the IP Security Policy snap-in or IPSECPOL.EXE/IPSECCMD.EXE to configure IPSec settings on a system.
W8.09	S	Use Group Policy to configure IPSec settings on computers automatically.
W8.10	K	Define Kerberos and how it works
W9		Backup and Disaster Recovery
W9.01	K	Define "disaster recovery."
W9.02	K	Describe the importance of multiple backups and off-site storage.

Windows Data		
W9.03	K	Describe the user rights necessary to backup and restore files on NTFS volumes.
W9.04	K	Define "system state", especially with regard to domain controllers.
W9.05	S	Use the Windows Backup program (or similar) to back up files and the system state.
W9.06	K	Describe Safe Mode and the Recovery Console.
W9.07	S	Boot a computer using the Recovery Console.
W9.08	S	Boot a computer into Safe Mode.
W9.09	K	Describe how to boot into Directory Services Restore Mode on a domain controller.
W9.10	K	Define "authoritative restore" as this pertains to domain controllers.
W9.11	S	Perform an authoritative restore of Active Directory on a domain controller.
W9.12	K	Describe the Emergency Repair Disk and its uses.
W9.13	S	Create an Emergency Repair Disk.
W9.14	K	Define "EFS recovery agent private key."
W9.15	K	Describe risks of Emergency Repair temporary directories
W9.16	K	Describe how the private key for the Encrypting File System (EFS) recovery agent certificate can be used to decrypt EFS-encrypted files on users' computers.
W9.17	S	Configure all the computers in a domain to use a different EFS recovery agent certificate using Group Policy.
W9.18	S	Back up the EFS recovery agent's private key using the Certificates MMC snap-in.
W9.19	S	Use REGEDT32.EXE or REGEDIT.EXE to back up and restore registry keys

UNIX Data		
U1		**Background Knowledge: Terms, Concepts and Tools**
U1.01	K	DESCRIBE the Unix process model
U1.02	S	USE standard commands to track Unix processes and an editor to edit files
U1.03	K	DESCRIBE the UNIX file system, including partitioning, swap space, and race conditions
U1.04	K, S	DESCRIBE and PERFORM Basic UNIX commands
U1.05	S	DEMONSTRATE knowledge of standard file directory locations under different flavors of UNIX
U1.06	S	DESCRIBE and UTILIZE the X Windows System (including adding and subtracting processes from the system boot process) and DESCRIBE the security implications of the X Windows System (xhost, .Xauthority files, etc) and how to use SSH for X tunneling
U1.07	S	DESCRIBE and UTILIZE the UNIX editing utility (vi)
U1.08	S	DESCRIBE and PERFORM startup and shutdown, including rc/init scripts and chkconfig
U1.09	K	DESCRIBE the Unix set-UID, set-GID mechanism and discuss the security issues with set-UID scripts
U1.10	K	Explain what capabilities root access allows and why root access must be limited to a few users with strong security skills
U1.11	K	Explain what a buffer overflow is and how it can give root access
U2		**Administrative Skills**
U2.01	S	DESCRIBE and PERFORM from source installations, including make and makefiles, and configure scripts and their common options
U2.02	S	DESCRIBE and UTILIZE the commands to format, partition, mount, and unmount drives under UNIX

		UNIX Data
U2.03	S	DESCRIBE and UTILIZE commands that can be used to backup and restore system data (*i.e.*, tar, dd, cpio, dump, restore)
U2.04	S	DESCRIBE and UTILIZE the commands used to manage users and groups and demonstrate the ability to add, delete and disable (but not delete) user accounts
U2.05	K	DESCRIBE ntp; demonstrate understanding of server strata, drift, and significance of time sync with regard to logfiles
U2.06	S	INSTALL and configure ntp/xntp
U2.07	S	DESCRIBE how to use sudo to manage root access; also describe its shortcomings (*i.e.*, root shell "escape" sequences in common programs like less and vi)
U2.08	S	SET up a cron job and cron security
U2.09	K	DESCRIBE how to limit user disk space usage with quota, and memory and CPU utilization with ulimit; Also how to limit core files, limit processes on a per user basis, and limit open file descriptors on a per-process basis.
U2.10	K	DESCRIBE techniques for tuning common network kernel parameters for security (increasing the half-open connection queue and reducing the time outs, turning off IP forwarding, disabling ICMP redirects, lowering ARP cache timeouts, etc)
U3		**Basic Security**
U3.01	K	DESCRIBE auditing and logging associated with UNIX
U3.02	S	DESCRIBE and UTILIZE UNIX network configuration files and commands and list the boot sequence on your version of UNIX
U3.03	K	DESCRIBE Unix permission bits and umask
U3.04	S	IDENTIFY excessive permissions on filesystem objects
U3.05	S	LOCATE & inventory SUID and SGID files; explain their significance
U3.06	S	RECOVER lost Unix passwords by booting from OS media
U3.07	S	RESET normal users' forgotten Unix passwords; reset the root password using single-user-mode
U3.08	K	DESCRIBE how passwords are cryptographically protected in UNIX; explain shadow password file
U3.09	K	DESCRIBE a method to force regular password changes and the limitations of the method
U310	K	DESCRIBE the purpose and potential risks associated with .rhosts and hosts.equiv
U311	K	DESCRIBE how to validate the integrity of a (downloaded) file using PGP/GPG signatures and/or md5 checksums
U312	K	DESCRIBE Kerberos authentication -- both one-time password authentication (and know what two-factor authentication is) as well as public-key based authentication systems
U313	S	CHANGE the hostname and/or IP address of a system manually (without re-installing the OS) after the system has been installed and been in production.
U314	K	DESCRIBE how to automate the creation of multiple essentially similar machines via Jumpstart or Kickstart or by "cloning" a machine from backup tapes.
U315	K	DESCRIBE how to find the latest complete set of security patches for your version of UNIX
U316	S	Download, install and verify a security patch or upgrade
U4		**Service-Specific Secure Configuration**
U4.01	S	DESCRIBE how to do basic DNS administration including updating zone files and debugging name resolution issues
U4.02	K	DESCRIBE DNS (BIND) and the secure management of DNS (*i.e.* chrooting, reverse lookups, changing version ID of the running name server, restricting zone transfers and recursive queries, setting up DNS forwarding)
U4.03	K	SET UP certificates for SSL communications
U4.04	S	CONFIGURE Apache for chroot operation; demonstrate understanding of httpd.conf access control options
U4.05	S	CONFIGURE FTP (wu_ftp or ProFTPD, for example) for secure operation including

UNIX Data		
		chroot, Anonymous, Guest (Restricted UID), etc., and secure execution (unprivileged group, etc)
U4.06	K	DESCRIBE the inetd.conf and xinetd.conf files to enable/disable services
U4.07	S	SECURELY CONFIGURE the inetd.conf/xinetd.conf file(s)
U4.08	K	DESCRIBE sendmail and how to prevent "spam" relaying; include use of smrsh for executing programs in a restricted environment; list the latest sendmail security features
U4.09	K	DESCRIBE nfs and its security implications
U410	K	DESCRIBE NIS and NIS security challenges
U411	K	DESCRIBE RPC security threats such as portmapper attacks and insecure RPC services such as rpc.cmsd, rpc.ttdbserverd
U412	K/S	DESCRIBE and INSTALL/USE TCP Wrappers program to allow mail filtering
U5		**Auditing/Prevention Methods**
U5.01	S	EMPLOY lsof AND/OR netstat to identify files and processes in use
U5.02	S	CONFIGURE logging via central syslog host; explain facilities and severities and how to tune message output for most useful data
U5.03	S	DEMONSTRATE how to close off network syslog access on machines that are not logging servers
U5.04	K	DESCRIBE the key log files on a UNIX system that should be regularly audited
U5.05	S	CONFIGURE swatch/logcheck to monitor logfiles for critical events and send appropriate notifications
U5.06	S	DESCRIBE syslog and explain how the different log levels can be used to enhance security monitoring
U5.07	S	CREATE logon/legal banner messages for all organizational & network access
U5.08	K	DESCRIBE Unix ACL permissions if your version of UNIX allows such control.
U5.09	S	DEMONSTRATE ability to create a forensic-grade image of a Unix system suitable for law-enforcement analysis
U5.10	K/S	DESCRIBE and INSTALL/USE Tripwire
U5.11	S	DEMONSTRATE configuration and enabling of system level accounting
U5.12	S	DEMONSTRATE configuration and enabling of process accounting
U5.13	S	DEMONSTRATE configuration and enabling of Kernel-level auditing
U6		**Specific Security Tools**
U6.01	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Crack or John the Ripper
U6.02	K/S	DESCRIBE and INSTALL/CONFIGURE/USE TARA
U6.03	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Sniffit or another sniffer
U6.04	S	DEMONSTRATE the ability to use PGP to send and receive signed and encrypted email
U6.05	S	DEMONSTRATE the ability to install and configure a host-based firewall (IP Tables/Chains under Linux or ipf on other UNIX flavors
U6.06	S	DEMONSTRATE the use of Bastille Linux, YASSP, or TITAN to harden UNIX Linux systems before deployment
U6.07	K/S	DESCRIBE and INSTALL/CONFIGURE/USE TCPDump
U6.08	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Secure Shell
U6.09	K/S	DESCRIBE and INSTALL/CONFIGURE/USE Nessus
U6.10	K/S	DESCRIBE and INSTALL/CONFIGURE/USE NMAP
U6.11	K/S	DESCRIBE and INSTALL/CONFIGURE/USE PortSentry

ANNEX B

REFERENCES

The following references pertain to this Instruction:

1. DODD 8000.1, Management of Information Resources and Information Technology, 27 Feb 02
2. DoDD 8500.1, Information Assurance, 24 Oct 02
3. DoDD 8500.1-M, Information Assurance Manual, (when effective)
4. DoD I 8500.2, Information Assurance (IA) Implementation, 6 Feb 03
5. DODI 5200.40, DITSCAP, 30 Dec 97
6. EO 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, 3 Apr 84
7. E O 13231, Critical Infrastructure Protection in the Information Age, 16 Oct 01
8. FIPS 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, Jun 74
9. FIPS Publication 65, Guideline for Automatic Data Processing Risk Analysis, 1 Aug 3
10. FIPS Publication 87, Guidelines for ADP Contingency Planning, 27 Mar 81
11. FIPS Publication 101, Guideline for Life Cycle Validation, Verification, and Testing of Computer Software, 6 Jun 83
12. FIPS Publication 102, Guideline for Computer Security Certification and Accreditation
13. NCSC TG-005, Trusted Network Interpretation (TNI), 31 Jul 87
14. NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems
15. NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
16. NIST SP 800-4, Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials, Mar 92
17. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, Oct 95
18. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, Sep 96
19. NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-based Model, Apr 98
20. NIST SP 800-18, Guide for Development of Security Plans for Information Technology Systems, Dec 98
21. NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, 1 Apr 92

22. NSTISSD 501, National Training Program for Information Systems Security (INFOSEC) Professionals, 16 Nov 92
23. NSTISSI No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), Apr 00
24. NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary, 19 May 2003
25. OMB Circular No. A-123, Management Accountability and Control, 21Jun 95
26. OMB Circular No. A-130, Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources, 30 Nov 00
27. OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, 28 Feb 00
28. OMB Memorandum M-01-08, Guidance on Implementing the Government Information Security Reform Act, 16 Jan 01.
29. OMB Memorandum M-01-24, Reporting Instructions for the Government Information Security Reform Act, 22 Jun 01.
30. OMB Memorandum M-02-01, Guidance for Preparing and Submitting Security Plans of Action and Milestones, 17 Oct 01.
31. OPM, 5 Combined Federal Regulation (CFR) Part 930, Training Requirements for the Computer Security Act, 3 Jan 92
32. PL 93-579, 5 U.S.C. 552a, the Privacy Act of 1974 (5 U.S.C. 552a)
33. PL 107-347, E-Government Act 0f 2002, Title III, Federal Information Security Management Act (FISMA), 17 Dec 02
34. PL 100-235, Computer Security Act of 1987, 8 Jan 88 and as amended by the Computer Security Enhancement Act of 1997, 11 Feb 97
35. PL 100-503, the Computer Matching and Privacy Protection Act
36. PL 104-106, Division E, the Information Technology Management Reform Act (Clinger-Cohen Act) of 1996
37. PL 106-398, Title X, Subtitle G, the Government Information Security Reform Act (GISRA)
38. The President's National Strategy to Secure Cyberspace, Feb 03